



ДиалОгНаука

SAFE
TECH
LAB



SafeTech CA

РОССИЙСКИЙ КОРПОРАТИВНЫЙ
ЦЕНТР СЕРТИФИКАЦИИ

SafeTech Group

Технологический лидер в создании современных инструментов безопасности для обеспечения цифрового доверия в инфраструктуре и онлайн-сервисах на базе средств криптографической защиты информации



Более
14 лет опыта



Клиенты — более
80 банков в РФ и СНГ



10 из ТОП 10
банков РФ



15 индустриальных
наград



Лучших поставщиков
ИБ-услуг в РФ



Сертификаты применяются повсеместно в инфраструктуре любого масштаба:

VPN сервисы

E-mail

Аутентификация
пользователей

Взаимодействие
оборудования

Доменные сервисы

Шифрование данных

Mutual TLS (mTLS)

И многое другое



Внешнее давление

- Microsoft приостановил деятельность на территории России
- SSL.COM, LET'S ENCRYPT, ZERO SLL поступили аналогично
- Блокирующие санкции и риски невыполнения требований по импортозамещению

VS



Гетерогенный IT-ландшафт

- Машины на Windows / MacOS / Linux
- iOS / Android — устройства
- Софт собственной разработки
- Железо и софт от разных производителей



SafeTech CA

кроссплатформенный сервис
для выпуска и управления
**технологическими
сертификатами**

 **минцифры_**
НОМЕР В РЕЕСТРЕ: **26307**

ЛЕГКО И ПРИВЫЧНО

Выпуск и управление
жизненным циклом
сертификатов

Поддержка **зарубежной**
(RSA, ECDSA, EdDSA) и
отечественной криптографии
(ГОСТ) на базе КриптоПро CSP

Создание иерархии PKI:
добавление корневых /
промежуточных /
выпускающих CA

Наличие **REST API**, поддержка
стандартных enrollment-
протоколов

Сеть точек публикации
CRL/AIA

Поддержка хранения ключей
CA в **HSM**

Поддержка **OCSP**

Публикация в **LDAP**

ЕЩЕ УДОБНЕЕ

Удобный **web-интерфейс**
администрирования

Мониторинг состояния
инстанса СА и его компонентов
онлайн в web-интерфейсе ЛК

Личный кабинет
Пользователя

Поддержка **согласования** в
процессе выпуска
сертификатов

Встроенные **инструменты**
миграции с MS CA

Настраиваемые **email-**
рассылки уведомлений

Формирование
отчетности

Широкая поддержка
протоколов **MS-WSTEP, SCEP,**
SSH, ACME, CMP, EST

ПЛАТФОРМЫ

Операционные системы



Мобильные устройства



Сетевое оборудование (стандарт IEEE 802.1x)



Другие платформы

ПРОТОКОЛЫ

MS-WSTEP

Полноценная замена
Microsoft CA

SCEP

Работа с MacOS, iOS,
Android, Linux, Cisco

SSH

Сертификаты для
безопасного удаленного
доступа

ACME

TLS для веб-порталов,
Kubernetes, Openshift

EST

Системы MDM

CMP

Базовый стандарт для API
OpenSSL, Bouncy Castle,
Nexus и других

Операционные системы

- Windows
- Linux, включая отечественные Astra Linux, ОС Альт, РЕД ОС, ОСнова, РОСА

Среда

- Java 21+

СУБД

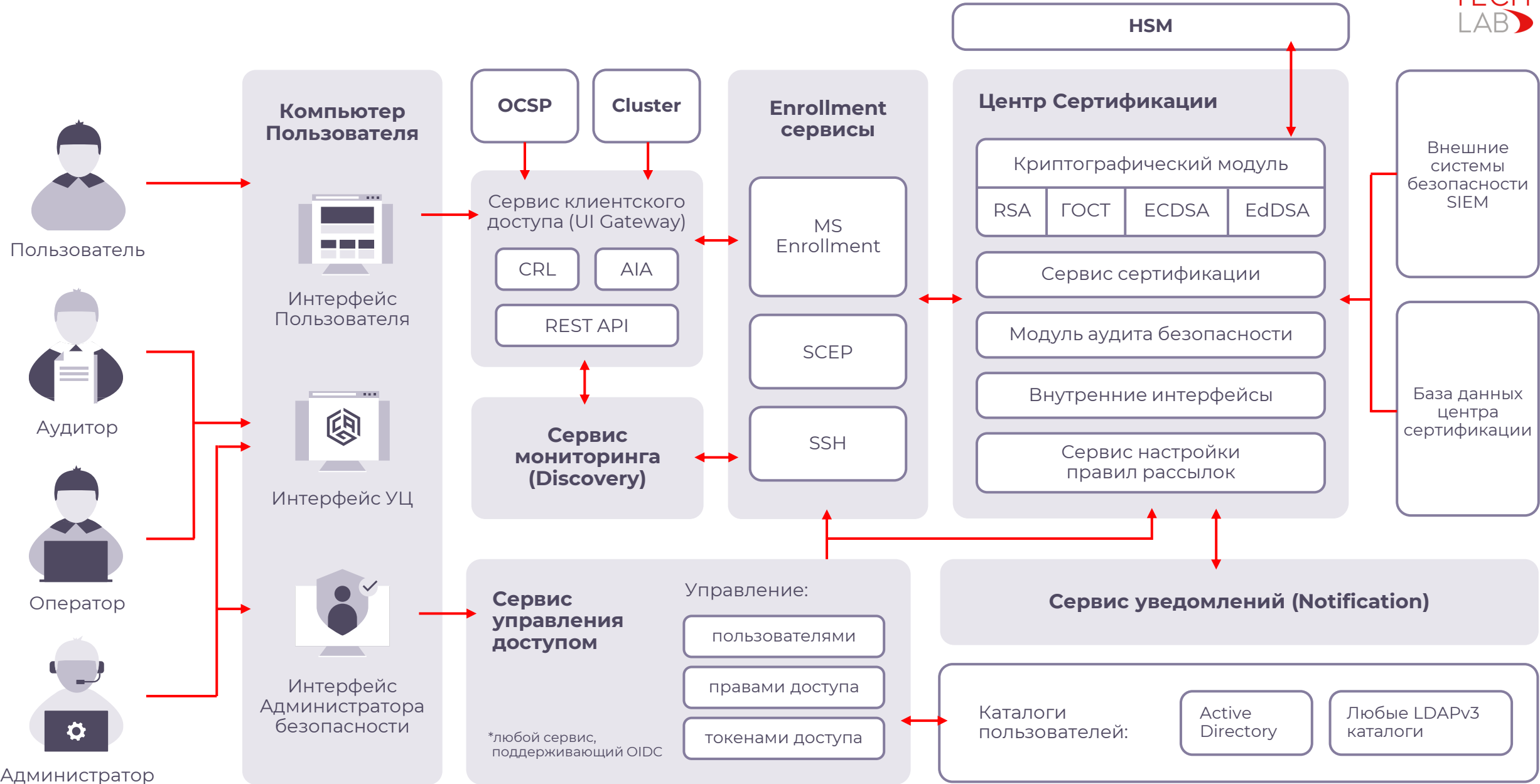
- Поддержка использования СУБД PostgreSQL для управления базами данных SafeTech CA, включая поддержку Postgres Pro Standard и Postgres Pro Certified

Развертывание

- Классическая виртуализация (VMware, KVM, Hyper-V и т.д.);
- Контейнерная виртуализация (Docker, OpenShift/K8S);
- Установка на физические сервера

Нагрузочное тестирование

- Тестирование на ОС Linux (стенд 2 CPU, 8 Gb RAM, 60 HDD)
- Выпуск **1500 сертификатов в минуту** при однопоточной нагрузке
- Стабильная работа на показателях ~ **700 000** выпускаемых сертификатов и **> 100 000** отозванных сертификатов



ROADMAP



2FA — ГОТОВЫЙ КЕЙС

ALD Pro

- PKINIT и интеграция с ST CA
- Раскатка софта, корневых и настроек

ST CA

- Управление сертификатами для SC Logon
- Личный кабинет пользователя и APM Администратора для работы с токенами из веб-интерфейса

Рутокен Логон

- PKINIT и интеграция с ALD Pro
- UI для входа в домен на Astra Linux

Рутокен KeyBox

- Полный цикл управления токенами в связке с ALD Pro

Рутокен
Enterprise
Logon



Инстанс SafeTech CA включает в себя:

- **Основные сервисы**
(CA core, Gateway, Discovery service, CRL/AIA services, OCSP, Notification service)
- **Стандартный интеграционный REST API**



Модуль MS Enrollment

обеспечивает поддержку управления сертификатами для пользователей MS Active Directory и компьютеров MS Windows



Модуль SSH

обеспечивает поддержку выпуска SSH-ключей



Модуль SCEP

обеспечивает поддержку управления сертификатами для сетевых устройств и ПО (Cisco, MS Intune, Linux, Mac, iOS и т.д.)



Модуль ACME

обеспечивает поддержку открытого интернет-стандарта ACME (Kubernetes, Openshift, Let's Encrypt)



Модуль КриптоПро

обеспечивает выпуск сертификатов с использованием криптографического ядра КриптоПро (ГОСТ, RSA, ECDSA)



Модуль CMP

базовый стандарт для API OpenSSL, Bouncy Castle, Nexus и других



4 **месяца**
срок пилота

2 **месяца**
срок проекта

2 **больших**
контура
сервисов СА

>10000
сертификатов



Команда специалистов Т-Банка показала экспертизу экстра класса



За время пилотирования было обнаружено и исправлено несколько багов в продукте



Roadmap продукта значительно наполнился «на вырост»



РЕЗУЛЬТАТЫ ПРОЕКТА



Внутренний контур
(включая Росбанк)
полноценно работает
в продакшн



Внешний контур
работает в продакшн
(выпуск TLS
сертификатов для
контрагентов)



MS CA отключен
от выпуска новых
сертификатов
(оставлен только
CRL)



Все новые
сертификаты
выпускаются
на **SafeTech CA**

УДОБНЫЙ И ФУНКЦИОНАЛЬНЫЙ UI



SafeTech CA

back: v3.1.2+build.1924
ui: v3.0.0+build.13

SafeTech-ROOT

Py

ca-standalone-admin
Администратор

Истекающие сертификаты

шаг: месяц

Сертификаты

Запросы

1

2

3

4

5

6

7

8

9

10

11

12

13

14

7

Всего

Активные

Приостановленные

Отозванные

Истекие

4

1

1

1

Мониторинг точек УЦ

GATEWAY

SSH

OCSP

CES

SCEP

DISCOVERY

NOTIFICATOR

CA CORE

УЦ

Лицензия

CRL

Delta CRL

Дата выдачи

Срок действия сертификата

Кем выдан

Организация

Серийный номер

Алгоритм подписи

25.03.2025

23.03.2035

SafeTech-ROOT

SafeTech-ROOT

0195ced06ff

SHAS12withRSA

Скачать сертификат

SafeTech CA

back: v3.1.2+build.1924
ui: v3.0.0+build.13

SafeTech-ROOT

Py

ca-standalone-admin
Администратор

CA

SSH

Мониторинг событий

ID события	Пользователь	IP пользователя	Тип события	Результат	Инфо
f885c5cc-80f5-4a32-b594-fa9708490...	anonymousUser	0.0.0.0:0.0:1	Get root certificate info	✓	1
89798340-c5ab-4fdf-bb1d-5a32ace65...	anonymousUser	10.0.32.107	Get root certificate info	✓	1
adbcd849-97e3-4f1c-bc75-695d674ea...	anonymousUser	10.0.32.107	Get root certificate info	✓	1
30151 99717af3-642d-4a4b-847f-c80dbe9c...	anonymousUser	10.0.32.67	Get root certificate info	✓	1
86f9e65d-4733-4af8-9f5d-961410e8d...	anonymousUser	10.0.32.71	Get root certificate info	✓	1
699195ec-077c-4b98-8496-a1430d54...	anonymousUser	10.0.32.167	Get root certificate info	✓	1
76d6466c-4d1a-4a9b-b7c1-8a602973...	anonymousUser	0.0.0.0:0.0:1	Get root certificate info	✓	1
e88133bb-837d-44a4-87fa-9fcc471c0...	anonymousUser	10.0.32.226	Get root certificate info	✓	1
09009a3d-fb24-436c-8006-c5a45b9d...	ca-standalone-admin	10.0.0.2	Get statistics by outOfDate batch	✓	1
75e2b761-fb43-4748-841a-cd05dbb47...	ca-standalone-admin	10.0.0.2	Get statistics by certificate status	✓	1

SafeTech CA

back: v3.1.2+build.1924
ui: v3.0.0+build.13

SafeTech-ROOT

Py

ca-standalone-admin
Администратор

CA

SSH

Импортировать шаблоны

Добавить шаблон

Web server ST-CA

Sub CA

User ST-CA

Test

Новый шаблон от 2025-07-17_201553

SCEP-Default

Web server for MS_ENROLLMENT

OCSP Signing

Новый шаблон от 2025-07-18_16:02:39

Новый шаблон

Тип протокола

Максимальный срок действия се...

Минимальная длина ключа

Использование ключа

Подпись

Шифрование данных

Подпись отписок отозванных сертификатов

Неотрекаемость от авторства

Согласование ключей

Зашифрование

Шифрование ключей

Подпись сертификатов ключей

Расшифрование

Использовать значения из шаблона

Всегда проверять уникальность публичного ключа

Обязательные имена субъекта

Роли шаблона

Администратор

Чтение

Запись

Выпуск

Автовыпуск